US005371797A

United States Patent [19]

Bocinsky, Jr.

[11] Patent Number: 5,371,797

[45] Date of Patent: Dec. 6, 1994

[54] **SECURE ELECTRONIC FUNDS TRANSFER FROM TELEPHONE OR UNSECURED TERMINAL**

[75] Inventor: **Ronald V. Bocinsky, Jr.**, Woodstock, Ga.

[73] Assignee: **Bellsouth Corporation**, Atlanta, Ga.

[21] Appl. No.: **5,350**

[22] Filed: **Jan. 19, 1993**

[51] **Int. Cl.**[5] **H04L 9/32**

[52] **U.S. Cl.** **380/24**; 340/825.34

[58] **Field of Search** 380/23–25, 380/825.34

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,023,013	5/1977	Kinker	380/24 X
4,123,747	10/1978	Lancto et al.	380/24 X
4,315,101	2/1982	Atalla	380/24 X
4,453,074	6/1984	Weinstein	380/24 X
4,747,050	5/1988	Brachtl et al.	380/24 X
4,965,568	10/1990	Atalla et al.	380/24 X
5,168,519	12/1992	Scarinci et al.	380/6
5,283,829	2/1994	Anderson	380/24

OTHER PUBLICATIONS

Network Interchange Security Systems User's Manual, Feb. 1991, Published by Atalla Network Security Systems.

Primary Examiner—Gilberto Barrón, Jr.

Attorney, Agent, or Firm—Jones & Askew

[57] **ABSTRACT**

A secure electronics funds or other financial transaction system that provides substantially equivalent security to that obtained by the use of secure point of sale terminals such as automatic teller machines, yet is conducted from unsecure terminal devices such as telephones, is disclosed. A customer registers himself or herself personally, together with information on his or her bank account at a secure transaction processor. A secure terminal is used to generate an encrypted version of a personal identification number (PIN) and provides the encrypted PIN and to the secure transaction processor. The encryption key used during encryption of the PIN is also acquired from either a specific request to, or monitoring data passing from a conventional network security transaction processor. The encrypted PIN is parsed with one portion being stored in the customer record at the secure transaction processor and the other being partially masked and provided back to the customer as an access code. Upon conducting a transaction, the customer provides the access code, which is unmasked and concatenated with second portion to recreate the original full encrypted PIN. This, together with the encryption key used for the original encryption is provided to conventional security and transaction processing apparatus for regional banking networks to seek authorization for the transaction.

9 Claims, 4 Drawing Sheets